C.n DevID uses in Smart Grid

Both AMI (Advanced Metering Infrastructure) and SCADA (Supervisory Control and Data Acquisition) systems would benefit from the separation of Domains of Trust provided by DevID. Frequently, although the utilities control which supplier's devices are in their networks, these devices are installed by independent contractors from their own inventory. On installation, the iDevID can validate that the device is from an approved list. The device supplier can track where their devices are used and work with the utility to ensure the software is current. The iDevID can be used to validate the safety of installing any software updates. This can even be carried to the point that the installation is not complete until the software is brought up to current levels.

The utilities take 'possession' of the device through the contractor run installation process to install an lDevID from their own PKI. All security operations on the utility network is authenticated via this lDevID. This prevents rogue devices, even from authorized suppliers, from functioning on the utility network. It provides the utility with a strong control over device configuration, separate from the supplier's control over installable software.

C.n DevID uses in ITS (Intelligent Transportation Systems)

ITS Infrastructure providers are typically governmental units. The infrastructure devices they deploy and manage are similar to the utility Smart Grid SCADA systems. Thus the use of DevID in these networks would mirror that in Smart Grid.

DevID in intelligent vehicles present a more complex opportunity. All the devices within a vehicle need to authenticate internally without any back end connection. lDevID is ideal for this purpose. Further it puts controls on what devices can be added to a vehicle after initial build (i.e. repairs and field enhancements) as these devices will have to connect to the back end services to acquire their lDevID. iDevID puts controls on what devices can even be installed in a vehicle, thus providing controls by the vehicle manufacturers on the certification of authorized devices in aftermarket situations. Device software updates can be authenticated by the iDevID and device configuration controlled by the lDevID.

A further level of lDevID may come from 3rd-party ITS applications that span ITS infrastructures and/or intelligent vehicle manufacturers. These 3rd-parties may provide their own PKI and issue their own lDevIDs to registered devices, leveraging the device's 'base' lDevID to authenticate the 3rd-party registration.